What is claimed is:

1. An information processing method in a center system, comprising:

receiving a first digital signature for specific data and data concerning a first user to be allowed to read said specific data, from a terminal of a second user;

comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

if it is judged that said first signature and said second signature are identical, performing a processing for enabling said first user to read said specific data.

2. The information processing method as set forth in claim 1, wherein said performing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, to a terminal of said first user.

3. The information processing method as set forth in claim 1, further comprising:

if it is judged that said first signature and said second signature are not identical, generating second hash data from said first digital signature;

comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said specific data; and

executing a processing for enabling said first user to read said specific data.

4. The information processing method as set forth in claim 3, wherein said executing comprises transmitting hash data, which is registered

in said data storage unit so as to correspond to said specific data, to a terminal of said first user.

5. An access authority management method in a center system, comprising:

receiving a first digital signature for specific data from a terminal of a user;

comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

if it is judged that said first digital signature and said second digital signature are identical, carrying out a setting to grant said user an authority to update said specific data.

6. The access authority management method as set forth in claim 5, further comprising:

if it is judged that said first digital signature and said second digital signature are not identical, generating first hash data from said first digital signature;

comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said specific data; and

if it is judged that said first hash data and said second hash data are identical, carrying out a setting to grant said user an authority to read said specific data.

7. The access authority management method as set forth in claim 6, further comprising transmitting an access denial notice to said terminal of said user, if it is judged that said first hash data and said second hash data are not identical.

8. The access authority management method as set forth in claim 5,

further comprising:

if data for updating said specific data is received from said terminal of said user, generating third hash data for the updated specific data;

transmitting said third hash data to said terminal of said user;

receiving a third digital signature generated from said third hash data, from said terminal of said user; and

registering said updated specific data, said third hash data, and said third digital signature into said data storage unit.

9. The access authority management method as set forth in claim 8, further comprising:

generating fourth hash data from said third digital signature before said registering; and

comparing said fourth hash data with said third hash data, and

wherein said registering is executed if it is judged that said fourth hash data and said third hash data are identical.

10. The access authority management method as set forth in claim 6, further comprising, if said authority to read said specific data is granted to said user, transmitting said specific data in a state where only reading is enabled, to said terminal of said user.

11. A data registration method in a center system, comprising:

if specific data is received from a user terminal, generate hash data for said specific data;

transmitting said hash data to said user terminal;

receiving a digital signature generated from said hash data; and

registering said specific data, said hash data and said digital signature into a data storage unit.

12. A data access method in a user system, comprising:

generating a digital signature from hash data, which is stored in a hash storage, for specific data;

transmitting an access request including said digital signature to a server; and

if said digital signature and a second digital signature, which is registered in said server, for said specific data are identical, receiving and displaying on a display device, said specific data in a state where updating is enabled, from said server.

13. The data access method as set forth in claim 12, further comprising, if said digital signature and said second digital signature, which is registered in said server, for said specific data are not identical, but hash data generated from said digital signature and second hash data, which is registered in said server, for said specific data are identical, receiving and displaying on a display device, said specific data in a state where only reading is enabled, from said server.

14. A computer program embodied on a medium, said computer program comprising:

receiving a first digital signature for specific data and data concerning a first user to be allowed to read said specific data, from a terminal of a second user;

comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

if it is judged that said first signature and said second signature are identical, performing a processing for enabling said first user to read said specific data.

15. The computer program as set forth in claim 14, wherein said

performing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, to a terminal of said first user.

16. The computer program as set forth in claim 14, further comprising:

if it is judged that said first signature and said second signature are not identical, generating second hash data from said first digital signature;

comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said specific data; and

executing a processing for enabling said first user to read said specific data.

17. The computer program as set forth in claim 16, wherein said executing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, to a terminal of said first user.

18. A computer program for an access authority management, said computer program comprising:

receiving a first digital signature for specific data from a terminal of a user;

comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

if it is judged that said first digital signature and said second digital signature are identical, carrying out a setting to grant said user an authority to update said specific data.

19. The computer program as set forth in claim 18, further comprising:

if it is judged that said first digital signature and said second digital signature are not identical, generating first hash data from said first digital signature;

comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said specific data; and

if it is judged that said first hash data and said second hash data are identical, carrying out a setting to grant said user an authority to read said specific data.

20. The computer program as set forth in claim 19, further comprising transmitting an access denial notice to said terminal of said user, if it is judged that said first hash data and said second hash data are not identical.

21. The computer program as set forth in claim 18, further comprising:

if data for updating said specific data is received from said terminal of said user, generating third hash data for the updated specific data;

transmitting said third hash data to said terminal of said user;

receiving a third digital signature generated from said third hash data, from said terminal of said user; and

registering said updated specific data, said third hash data, and said third digital signature into said data storage unit.

22. The computer program as set forth in claim 21, further comprising:

generating fourth hash data from said third digital signature before said registering; and

comparing said fourth hash data with said third hash data, and

wherein said registering is executed if it is judged that said fourth hash data and said third hash data are identical.

23. The computer program as set forth in claim 19, further comprising, if said authority to read said specific data is granted to said user, transmitting said specific data in a state where only reading is enabled, to said terminal of said user.

24. A center system, comprising:

means for receiving a first digital signature for specific data and data concerning a first user to be allowed to read said specific data, from a terminal of a second user;

means for comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

means for performing a processing for enabling said first user to read said specific data, if it is judged that said first signature and said second signature are identical.

25. The center system as set forth in claim 24, wherein said means for performing comprises means for transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, to a terminal of said first user.

26. The center system as set forth in claim 24, further comprising:

means for generating second hash data from said first digital signature, if it is judged that said first signature and said second signature are not identical;

means for comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said specific data; and

means for executing a processing for enabling said first user to read said specific data.

27. The center system as set forth in claim 26, wherein said means for executing comprises means for transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, to a terminal of said first user.

28. A center system, comprising:

means for receiving a first digital signature for specific data from a terminal of a user;

means for comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

means for carrying out a setting to grant said user an authority to update said specific data, if it is judged that said first digital signature and said second digital signature are identical.

29. The center system as set forth in claim 28, further comprising:

means for generating first hash data from said first digital signature, if it is judged that said first digital signature and said second digital signature are not identical;

means for comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said specific data; and

means for carrying out a setting to grant said user an authority to read said specific data, if it is judged that said first hash data and said second hash data are identical.

30. The center system as set forth in claim 29, further comprising means for transmitting an access denial notice to said terminal of said user, if it is judged that said first hash data and said second hash data are not identical.

31. The center system as set forth in claim 28, further comprising:

means for generating, if data for updating said specific data is received from said terminal of said user, third hash data for the updated specific data;

means for transmitting said third hash data to said terminal of said user;

means for receiving a third digital signature generated from said third hash data, from said terminal of said user; and

means for registering said updated specific data, said third hash data, and said third digital signature into said data storage unit.

32. The center system as set forth in claim 31, further comprising:

means for generating fourth hash data from said third digital signature before said registering; and

means for comparing said fourth hash data with said third hash data, and

wherein said means for registering operates if it is judged that said fourth hash data and said third hash data are identical.

33. The center system as set forth in claim 29, further comprising means for transmitting said specific data in a state where only reading is enabled, to said terminal of said user, if said authority to read said specific data is granted to said user.